IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Richard Paul TARQUINI
Serial No.:	10/003,747
Filing Date:	October 31, 2001
Group Art Unit:	2132
Examiner:	Perungavoor, Venkatanaray
Title:	METHOD, COMPUTER READABLE MEDIUM, AND NODE FOR A THREE-LAYERED INTRUSION PREVENTION SYSTEM FOR DETECTING NETWORK EXPLOITS
Docket No.:	10014006-1

MAIL STOP: APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

AMENDED APPEAL BRIEF

Applicant appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed August 3, 2005, finally rejecting Claims 1-19. Applicant filed a Notice of Appeal on October 3, 2005. Applicant respectfully submits herewith this Amended Appeal Brief.

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 21, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012751, Frame 0518. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-19 stand rejected pursuant to a Final Office Action mailed August 3, 2005. Claims 1-19 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a method of preventing intrusions on a node of a network (100) comprising: monitoring, by a first layer (110) of an intrusion prevention system (300), application data of applications running on the node; monitoring, by a second layer (110) of the intrusion prevention system (300), transport layer data of the node; and monitoring, by a third layer (140) of the intrusion prevention system (300), network layer data of the node. (at least at page 16, line 17 to page 18, line 28; and figure 6).

Embodiments of the present invention as defined by independent Claim 9 are directed toward a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor (272), cause the processor (272) to perform a computer method of: monitoring application layer data, by a first layer (110) of an intrusion prevention system (300) comprised of the instructions, of a node of a network (100), the node comprising the processor (272); monitoring transport layer data, by a second layer (110) of the intrusion prevention system (300), of the node of the network (100); and monitoring network layer data, by a third layer (140) of an intrusion prevention system (300), of the node of the network (100). (at least at page 12, line 26 to page 13, line 15; page 15, lines 1-14; page 16, line 17 to page 18, line 28; and figures 4-6).

Embodiments of the present invention as defined by independent Claim 17 are directed toward a node of a network (100) comprising a central processing unit (272), a memory module (274) for storing data in machine readable format for retrieval and execution by the central processing unit (272), and an operating system (275) comprising a network stack (90) comprising a protocol driver (135), a media access control driver (145), the memory module (274) storing an instance of an intrusion protection system (300) application (91) operable to monitor application layer data and an intrusion prevention system transport service provider layer (120), and the operating system (275) having an intrusion prevention system network filter service provider (140) bound to the media access control driver (145) and the protocol driver (135). (at least at page 12, line 26 to page 13, line 15; page 14, lines 3-19; page 15, lines 1-14; page 16, line 17 to page 18, line 28; and figures 4-6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 5-9 and 14-16 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*").

2. Claims 2, 3, 4, 10-13, 17-19 are rejected under 35 U.S.C. §103(a) as being unpatentable in view of U.S. Patent No. 6,279,113 to "*Vaidya*" in view of U.S. Patent No. 6,851,061 issued to Holland, III et al. (hereinafter "*Holland*").

ARGUMENT

A. Standard

1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed.

Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. First Ground of Rejection (Claims 1, 5-9 and 14-16)

Claims 1, 5-9 and 14-16 are rejected under 35 U.S.C. §102(e) as being anticipated by *Vaidya*. Of these claims, Claims 1 and 9 are independent. Applicants respectfully submit that each of independent Claims 1 and 9 is patentable over the cited references, and thus remaining Claims 5-8 and 14-16 that depend respectively from independent Claims 1 and 9 are also patentable.

Embodiments of the present invention generally involve a method for detecting network intrusions. For example, according to one embodiment of Applicants' invention, an intrusion prevention system (IPS) (300) comprises a three-layered IPS (300) installed in a protocol stack (90) (at least at page 16, lines 17-21; and figure 6). For example, in some embodiments of Applicants' invention, attack threat analysis is performed at three different layers of the protocol stack (90) (at least at page 16, lines 22-24; and figure 6). In such embodiments of Applicants' invention, an IPS application service provider layer (110) of the IPS (300) provides system integrity via baseline analysis of, for example, running programs, file systems, user profile management applications, monitoring of application logs to determine when an attack has occurred, network usage monitoring and other "log watching" measures and monitoring of an application layer (108) of the protocol stack (90) (at least at page 16, lines 23-27; and figure 6). The IPS application service provider layer (110) also facilitates operation of an IPS transport service provider

layer (120) and a network filter service provider (140) installed at the network layer of the protocol stack (90) as an intermediate driver of the network stack (90) (at least at page 16, lines 27-30; and figure 6). The IPS transport service provider layer (120) of the IPS (300) establishes a baseline of network ports, sockets, and network application usage and is preferably above any network encryption layer of the protocol stack (90) so that content scanning may be performed thereby on raw application data prior to the application data being encapsulated by a protocol driver (135) of the stack (90) for transmission across a network (100) (at least at page 17, lines 12-17; and figure 6). The network filter service provider layer (140) of the IPS (300) is bound to a media access control (MAC) driver (145) and protocol driver (135) at the network layer of the protocol stack (90) and thus performs low-level filtering comprising filtering for atomic network attacks, network protocol level attacks, IP filtering, port filtering and gathering of network statistics on both inbound and outbound directions (at least at page 17, line 29 to page 18, line 1; and figure 6). Thus, embodiments of the present invention detect and prevent inbound exploits from reaching upper layers of the network stack (90) by discarding frames identified as suspicious or intrusion-related at the network layer and prevent exploits originating from a node running IPS (300), such as exploitative data generated from a Trojan application disposed at an application layer (108), from being transmitted from the node running the IPS (300), thus preventing the node running the IPS (300) from being used as a zombie system in a network attack (at least at page 17, lines 11-17). Further, network exploits that circumvent network the filter service provider (140) of IPS (300), for example by bypassing signature analysis techniques employed thereby via multiframe or fragmented attacks or other means, are be detected by the transport service provider (120), and application level attacks are detected by the service provider layer (110). Accordingly, for example, independent Claim 1 recites "monitoring, by a first layer of an intrusion prevention system, application data of applications running at on the node; monitoring, by a second layer of the intrusion prevention system, transport layer data of the node; and monitoring, by a third layer of the intrusion prevention system, network layer data of the node.

In the Final Office Action, the Examiner states that *Vaidya* discloses "an intrusion detection system whereby all of the seven OSI layers are monitored" which, according to the Examiner, anticipates independent Claims 1 and 9 (Final Office Action, page 3). Applicants respectfully disagree. In the Final Office Action, the Examiner refers to column 4, lines 29-31 of *Vaidya* which recite:

> An advantage of the present invention is that all seven layers of the OSI model are monitored and so an attack based in any of the layers can be detected.

Applicant respectfully submits that the portion of *Vaidya* referred to by the Examiner, without more, does not rise to the level required to support a rejection under 35 U.S.C. § 102. For example, to support a rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131. Applicant respectfully submits that the portion of *Vaidya* referred to by the Examiner does not disclose or even suggest "monitoring, by a first layer of an intrusion prevention system, application data of applications running at on the node," "monitoring, by a second layer of the intrusion prevention system, transport layer data of the node" and "monitoring, by a third layer of the intrusion prevention system, network layer data of the node" as recited by Claim 1 (emphasis added), or "monitoring application layer data, by a first layer of an intrusion prevention system," "monitoring transport layer data, by a second layer of the intrusion prevention system" and "monitoring network layer data, by a third layer of an intrusion prevention system" as recited by Claim 9 (emphasis added). Therefore, for at least this reason, Applicant respectfully submits that *Vaidya* does not anticipate independent Claims 1 and 9.

Further, *Vaidya* recites that:

> The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application

> information from the data packet. Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model.

(*Vaidya*, column 7, lines 18-24). Applicants respectfully submit that extracting header information from a data packet retrieved from a queue is not the same as monitoring layer data by different layers of an intrusion prevention system as generally recited by Claims 1 and 9. Accordingly, for at least this reason also, Applicants respectfully submit that *Vaidya* does not anticipate Claims 1 and 9.

Accordingly, for at least the reasons discussed above, independent Claims 1 and 9 are clearly patentable over *Vaidya*. Therefore, Claims 1 and 9, and Claims 5-8 and 14-16 that depend respectively therefrom, are in condition for allowance.

2. Second Ground of Rejection (Claims 2-4, 10-13 and 17-19)

Claims 2-4, 10-13 and 17-19 are rejected under 35 U.S.C. §103(a) as being unpatentable in view of *Vaidya* in view of *Holland*. Claims 2-4 and 10-13 depend respectively from independent Claims 1 and 9. At least for the reasons discussed above, independent Claims 1 and 9 are allowable. Moreover, *Holland* does not appear to remedy at least the deficiencies of *Vaidya* indicated above, nor did the Examiner rely on *Holland* to reject independent Claims 1 and 9. Therefore, Applicant respectfully submits that Claims 2-4 and 10-13 are patentable over the cited references.

Of the remaining rejected claims, Claim 17 is independent. Applicant respectfully submits that independent Claim 17 is patentable over the cited references and, therefore, Claims 18 and 19 that depend therefrom, are also patenable.

Applicant respectfully submits that neither *Vaidya* nor *Holland*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 17. For example, independent Claim 17 recites "an operating system comprising a network stack comprising a protocol driver, a media access control driver . . . and an intrusion prevention system transport service provider layer" (emphasis added). The Examiner

appears to indicate that *Vaidya* does not disclose at least the above-referenced limitations of independent Claim 17 ("*Vaidya* discloses a [sic] processor, memory module . . . but does not disclose the use of drivers to monitor network layer, transport layer interface . . . ." (Final Office Action, page 6)). However, the Examiner also appears to indicate that *Holland* discloses such limitations (Final Office Action, page 6). Applicants respectfully disagree. *Holland* appears to disclose an internal protocol (IP) stack 33 for processing incoming data frames (*Holland*, column 4, lines 41-44, figure 2). *Holland* also appears to disclose, and the Examiner appears to refer to, a packet filter 37 of *Holland* used to collect all network traffic transiting through the NIC 31 of *Holland*, and an auditing system 34 for monitoring system-level activities (Final Office Action, page 6, *Holland*, column 4, lines 41-55, figure 2). However, neither the packet filter 37 nor the auditing system 34 of *Holland* appear to form any portion of "a network stack" (*see, e.g.*, figure 2 of *Holland* where the IP stack 33 of Holland is illustrated as a separate component from either the packet filter 37 or the auditing system 34 of *Holland*). Thus, *Holland* does not appear to disclose or even suggest "a network stack comprising a protocol driver, a media access control driver . . . and an intrusion prevention system transport service provider layer" as recited by independent Claim 17 (emphasis added), nor does the Examiner appear to explicitly identify any such disclosure in *Holland*. Moreover, *Vaidya* does not remedy at least this deficiency of *Holland*. Accordingly, for at least this reason, Applicant respectfully submits that neither *Vaidya* nor *Holland*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 17.

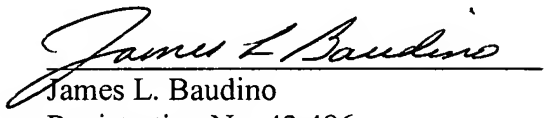
Accordingly, for at least the reasons discussed above, independent Claim 17 is clearly patentable over the cited references. Therefore, independent Claim 17, and Claims 18 and 19 that depend therefrom, are in condition for allowance.

CONCLUSION

Applicant has demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicant respectfully requests the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

Although no other fee is believed due with this Amended Appeal Brief, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,



James L. Baudino
Registration No. 43,486

Date: March 13, 2006

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884

CLAIMS APPENDIX

1. A method of preventing intrusions on a node of a network, comprising;

monitoring, by a first layer of an intrusion prevention system, application data of applications running at on the node;

monitoring, by a second layer of the intrusion prevention system, transport layer data of the node; and

monitoring, by a third layer of the intrusion prevention system, network layer data of the node.

2. The method according to claim 1, wherein monitoring network layer data of the node further comprises monitoring network layer data of the node by the third layer of the intrusion prevention system bound to a media access control driver and a protocol driver of an instance of a network stack of the node.

3. The method according to claim 1, wherein monitoring transport layer data of the node further comprises monitoring transport layer data of the node by the second layer of the intrusion prevention system bound to a transport driver interface of an instance of a network stack of the node.

4. The method according to claim 1, wherein monitoring application layer data of the node further comprises monitoring application layer data of the node by the first layer of the intrusion prevention system, the first layer interfacing with the second layer by a dynamically linked library.

5. The method according to claim 1 further comprises interfacing the first layer of the intrusion prevention system with a file system.

6. The method according to claim 5, wherein interfacing the first layer of the intrusion prevention system with a file system further comprises interfacing the first layer of the intrusion prevention system with a file system comprising at least one of an events-database for archiving intrusion-related events detected by the intrusion prevention

system, a report database for storing reports related to intrusion-related events detected by the intrusion prevention system and a signature file database.

7. The method according to claim 6, further comprising providing, by the first layer of the intrusion prevention system, one or more signature files maintained in the signature file database to the third layer of the intrusion prevention system.

8. The method according to claim 1, further comprising engaging a communication session between the first layer of the intrusion prevention system and a management client of an intrusion prevention system running on a second node of the network.

9. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

monitoring application layer data, by a first layer of an intrusion prevention system comprised of the instructions, of a node of a network, the node comprising the processor;

monitoring transport layer data, by a second layer of the intrusion prevention system, of the node of the network; and

monitoring network layer data, by a third layer of an intrusion prevention system, of the node of the network.

10. The computer readable medium according to claim 9, further comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of binding the third layer with a media access control driver and a protocol driver of an instance of a network stack running on the node.

11. The computer readable medium according to claim 10, wherein binding the third layer with a media access control driver and a protocol driver further comprises binding the third layer with the media access control driver and the protocol driver upon initialization of the network stack.

12. The computer readable medium according to claim 9, further comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of binding the second layer with a transport driver interface of an instance of a network stack running on the node.

13. The computer readable medium according to claim 12, wherein binding the second layer with a transport driver interface further comprises binding the second layer with the transport driver interface at initialization of the network stack.

14. The computer readable medium according to claim 9, further comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of communicating, by the first layer, with a file system.

15. The computer readable medium according to claim 9, further comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of communicating, by the first layer, with a management application running on a second node of the network.

16. The computer readable medium according to claim 14, further comprising a set of instructions that, when executed by a processor, cause the processor to perform a computer method of archiving intrusion related events detected by the intrusion protection system in a database of the file system.

17. A node of a network, comprising:

a central processing unit;

a memory module for storing data in machine readable format for retrieval and execution by the central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver, the memory module storing an instance of an intrusion protection system application operable to monitor application layer data and an intrusion prevention system transport service provider layer, and the operating system having an

intrusion prevention system network filter service provider bound to the media access control driver and the protocol driver.

18. The node according to claim 17, further comprising a file system, the intrusion protection system application operable to communicate with the file system.

19. The node according to claim 18, wherein the file system comprises a database, the intrusion prevention system application operable to log intrusion-related data in the database, the intrusion-related data obtained by at least one of the intrusion prevention system application, the intrusion prevention system transport service provider and the intrusion prevention system network filter service provider.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None